# SERVER MALWARE PROTECTION POLICY

**1. Overview**

Is an obligation for Kube to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

**2. Purpose**

The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

**3. Scope**

This policy applies to all servers that Kube and its partners are responsible to manage, including all server systems setup for internal use.

**4. Policy**

Kube Group staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

**4.1 ANTIVIRUS**

All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- NBT/Microsoft Share access is open to this server from systems used by non-administrative users
- HTTP/FTP access is open from the Internet

- Other “risky” protocols/applications are available to this system from the Internet at the discretion of the Pixie Services Security Administrator

All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

Outbound web access is available from the system

**4.2 MAIL SERVER ANTI-VIRUS**

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

**4.3 ANTI-SPYWARE**

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own

**5 Policy Compliance**

1.1 Compliance Measurement

Kube Group managers will verify compliance to this policy through various methods, including but not limited to, internal and external audits.

1.2 Exceptions

Any exception to the policy must be approved by Kube managers in advance.

1.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.